Avaya Solution & Interoperability Test Lab

Application Notes for VoSKY Exchange Pro VISIP-EX with Avaya Communication Manager and Avaya SIP Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration required for VoSKY Exchange Pro VISIP-EX to successfully interoperate with Avaya Communication Manager and Avaya SIP Enablement Services (SES). Exchange Pro VISIP-EX is a PBX to Skype™ gateway that connects to Avaya SES via a SIP connection and is used to route calls between the enterprise and the Skype Voice over IP (VoIP) network.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration required for VoSKY Exchange Pro VISIP-EX to successfully interoperate with Avaya Communication Manager and Avaya SIP Enablement Services (SES). Exchange Pro VISIP-EX is a PBX to Skype™ gateway that connects to Avaya SES via a SIP connection and is used to route calls between the enterprise and the Skype Voice over IP (VoIP) network.

1.1. Interoperability Compliance Testing

The interoperability compliance testing consisted of placing calls through the Exchange Pro and exercising common PBX features. Calls were placed between the Avaya Communication Manager endpoints and Internet users running a Skype client; as well as between the Avaya Communication Manager endpoints and the Skype-connected PSTN. Interoperability with all major enterprise phone types (analog, digital, H.323 and SIP) was tested. See **Section 7** for complete test results.

1.2. Support

Contact VoSKY technical support via the following methods:

Phone: 719-884-7417
On-Line: http://www.vosky.com/cms/index/support.php

2. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows the Exchange Pro at the enterprise connected to the enterprise IP network on one side and the public Internet on the other. The public Internet connection provides access to the Skype service which allows the Exchange Pro to connect to other Skype users and the PSTN.

Located at the enterprise site is an Avaya SES and an Avaya S8300 Server running Avaya Communication Manager in an Avaya G700 Media Gateway. Avaya IA 770 Intuity Audix is also running on the Avaya S8300 Server. Endpoints include an Avaya 4600 Series IP Telephone (with SIP firmware), Avaya 9600 Series IP Telephones (with SIP and H.323 firmware), an Avaya one-X Desktop Edition, an Avaya 6408D Digital Telephone, and an Avaya 6210 Analog Telephone.

Skype users do not have phone numbers but instead are addressed via an alphanumeric Skype ID. In order for PBX endpoints to call these users, the Exchange Pro maps the Skype ID to a number that the PBX user can dial. This mapping is stored in the Exchange Pro phonebook. Similarly, inbound calls from Skype to Exchange Pro are addressed not by a number but by one of several Skype IDs/accounts assigned to the Exchange Pro. The Exchange Pro uses its Skype IDs as a pool of resources for all incoming calls. Calls to any of the Skype IDs can be answered by another if the addressed Skype ID is busy. All calls to any of the Skype IDs are directed to Avaya SES. Since Skype does not provide a destination phone number, all calls from Exchange Pro are directed to a single number on Avaya Communication Manager. This number is typically the number of an automated attendant or other IVR application. This number is configurable on the Exchange Pro.

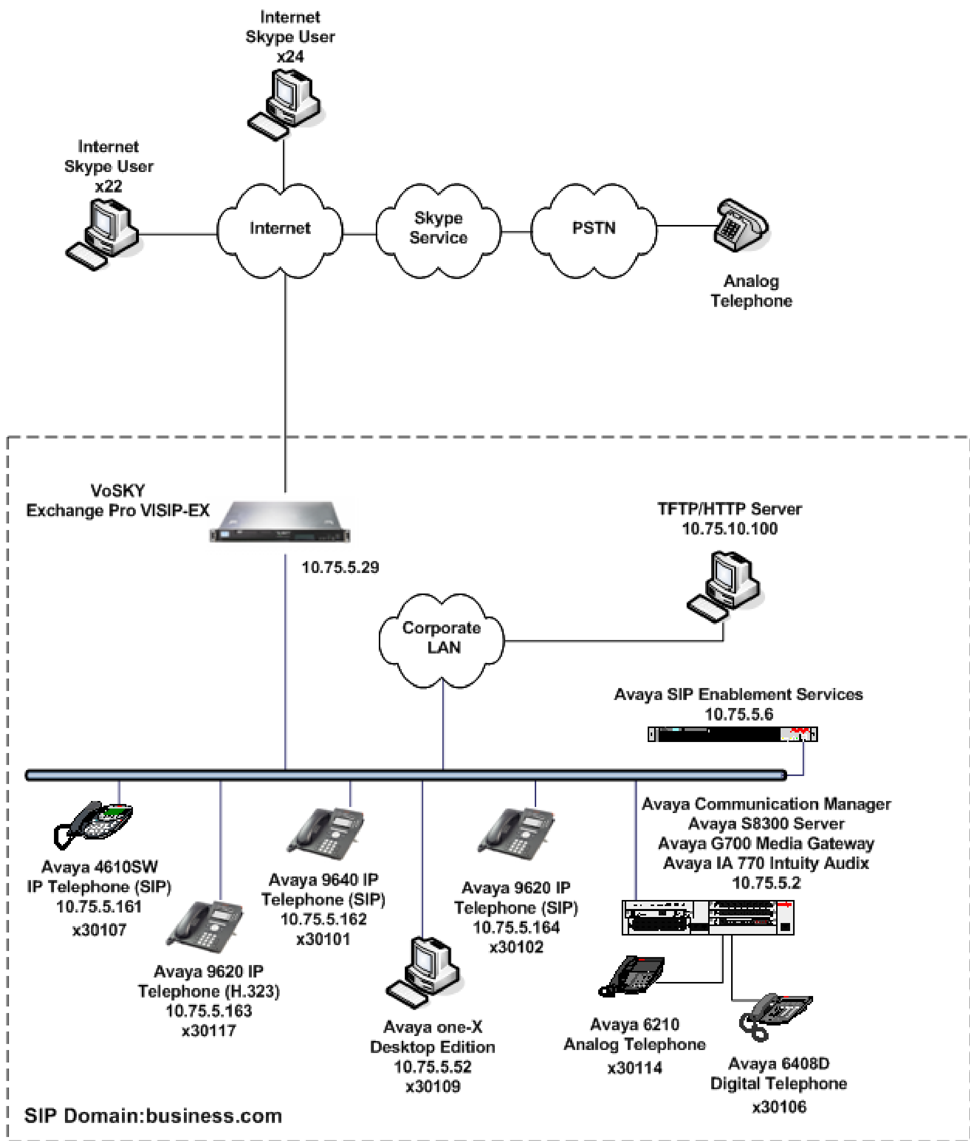


Figure 1: Exchange Pro VISIP-EX Test Configuration

3. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided.

Equipment	Software/Firmware
Avaya S8300B Server	Avaya Communication Manager 5.1.1 Service Pack (01.1.415.16402) with Avaya IA 770 Intuity Audix
Avaya G700 Media Gateway	MGP: 28.18.0 VOIP: 76
Avaya S8500B Server	Avaya SIP Enablement Services (SES) 5.1.1
Avaya 9620 IP Telephone (H.323)	Avaya one-X Deskphone Edition 2.0
Avaya 4610SW IP Telephones (SIP)	2.2.2
Avaya 9620 IP Telephones (SIP) Avaya 9640 IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 2.0.5
Avaya one-X Desktop Edition (SIP)	2.1 Service Pack 2
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
Analog Telephone	-
Windows PC (TFTP/HTTP Server)	Windows XP Professional SP2
VoSKY Exchange Pro VISIP-EX	1.0

4. Configure Avaya Communication Manager

This section describes the Avaya Communication Manager configuration to support the network shown in **Figure 1**. It assumes the procedures necessary to support SIP and connectivity to Avaya SES have been performed as described in [3]. This section also assumes that an Outboard Proxy SIP (OPS) off-PBX telephone mapping has been configured on Avaya Communication Manager for each SIP endpoint in the configuration as described in [3] and [4].

This section is divided into two parts. **Section 4.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. It will not attempt to show the installation procedures in their entirety. The section will also describe any deviations from the standard procedures, if any.

Section 4.2 will describe procedures beyond the initial SIP installation procedures that are necessary for interoperating with Exchange Pro. It will describe the SIP connection used by Avaya Communication Manager to route calls to Avaya SES bound for Exchange Pro.

The configuration of Avaya Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

4.1. Summary of Initial SIP Installation

This section summarizes the applicable user-defined parameters used during the SIP installation procedures.

Step	Description
1.	**IP network region** The Avaya S8300 Server, Avaya SES and IP (H.323/SIP) endpoints were located in a single IP network region (IP network region 1) using the parameters described below. Use the **display ip-network-region** command to view these settings. The example below shows the values used for the compliance test. ▪ The **Authoritative Domain** field was configured to match the domain name configured on Avaya SES. In this configuration, the domain name is ***business.com***. This name appears in the "From" header of SIP messages originating from this IP region. ▪ A descriptive name was entered for the **Name** field. ▪ **IP-IP Direct Audio** (shuffling) was enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. This was done for both intra-region and inter-region IP-IP Direct Audio. This is the default setting. Shuffling can be further restricted at the trunk level on the **Signaling Group** form. ▪ The **Codec Set** field was set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected. ▪ The default values were used for all other fields.

```
display ip-network-region 1                                        Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: business.com
    Name: Default
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Step	Description
2.	**Codecs** IP codec set 1 was used for the compliance test. Multiple codecs can be listed in priority order to allow the codec used by a specific call to be negotiated during call establishment. The list includes the codecs the enterprise wishes to support within the normal trade-off of bandwidth versus voice quality. The example below shows the values used in the compliance test. The Exchange Pro only supports G.711 mu-law. Thus, for testing purposes the IP codec set was limited only to ***G.711MU***.

```
display ip-codec-set 1                                          Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2:
 3:
```

Step	Description
3.	**Signaling Group** For the compliance test, signaling group 1 was used for the signaling group associated with the SIP trunk group between Avaya Communication Manager and Avaya SES. Signaling group 1 was configured using the parameters highlighted below. All other fields were set as described in [3]. ▪ The **Group Type** was set to ***sip***. ▪ The **Transport Method** was set to the recommended default value of ***tls*** (Transport Layer Security). As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to ***5061.*** ▪ The **Near-end Node Name** was set to ***procr***. This node name maps to the IP address of the Avaya S8300 Server. Node names are defined using the **change node-names ip** command. ▪ The **Far-end Node Name** was set to ***SES***. This node name maps to the IP address of Avaya SES as defined using the **change node-names ip** command. ▪ The **Far-end Network Region** was set to ***1***. This is the IP network region which contains Avaya SES. ▪ The **Far-end Domain** was set to ***business.com***. This is the domain configured on Avaya SES. This domain is sent in the "To" header of SIP INVITE messages for calls using this signaling group. ▪ **Direct IP-IP Audio Connections** was set to ***y***. This field must be set to ***y*** to enable media shuffling on the SIP trunk. ▪ The **DTMF over IP** field was set to the default value of ***rtp-payload***. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833. ▪ The default values were used for all other fields.

```
display signaling-group 1
                                SIGNALING GROUP

 Group Number: 1             Group Type: sip
                       Transport Method: tls



   Near-end Node Name: procr                 Far-end Node Name: SES
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1
       Far-end Domain: business.com

                                     Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
                                                       IP Audio Hairpinning? n
         Enable Layer 3 Test? n
 Session Establishment Timer(min): 3              Alternate Route Timer(sec): 6
```

Step	Description
4.	**Trunk Group** For the compliance test, trunk group 1 was used for the SIP trunk group between Avaya Communication Manager and Avaya SES. Trunk group 1 was configured using the parameters highlighted below. All other fields were set as described in [3]. On **Page 1**: ▪ The **Group Type** field was set to ***sip***. ▪ A descriptive name was entered for the **Group Name**. ▪ An available trunk access code (TAC) that was consistent with the existing dial plan was entered in the **TAC** field. ▪ The **Service Type** field was set to ***tie***. ▪ The **Signaling Group** was set to the signaling group shown in the previous step. ▪ The **Number of Members** field contained the number of trunks in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration. Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk. ▪ The default values were used for all other fields.

```
display trunk-group 1                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 1                   Group Type: sip           CDR Reports: y
  Group Name: SES Trk Grp                COR: 1        TN: 1        TAC: 101
   Direction: two-way       Outgoing Display? y
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n

                                                      Signaling Group: 1
                                                    Number of Members: 10
```

Step	Description

5.	**Trunk Group – continued**
	On **Page 3**:
	▪ The **Numbering Format** field was set to ***public***. This field specifies the format of the calling party number sent to the far-end.
	▪ The default values were used for all other fields.
	<pre>display trunk-group 1 Page 3 of 21
	TRUNK FEATURES
	          ACA Assignment? n Measured: none
	                                                      Maintenance Tests? y
	
	                     Numbering Format: public
	                                            UUI Treatment: service-provider
	
	                                             Replace Restricted Numbers? n
	                                            Replace Unavailable Numbers? n
	
	 Show ANSWERED BY on Display? y</pre>

6.	**Public Unknown Numbering**
	Public unknown numbering defines the calling party number to be sent to the far-end. Use the **display public-unknown-numbering** command to view the calling party entries. An entry was created for use by the trunk group defined in **Step 4**. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed across any trunk group (**Trk Grp** column is blank) will be sent as a 5-digit calling number. This calling party number is sent to the far-end in the SIP "From" header.
	<pre>display public-unknown-numbering 0 Page 1 of 2
	                      NUMBERING - PUBLIC/UNKNOWN FORMAT
	                                           Total
	Ext Ext Trk CPN CPN
	Len Code Grp(s) Prefix Len
	                                                     Total Administered: 1
	 5 3 **5** Maximum Entries: 240</pre>

4.2. Configure SIP Trunk and Routing to Exchange Pro VISIP-EX

To communicate to Exchange Pro, a second SIP trunk with the appropriate call routing must be configured on Avaya Communication Manager. This SIP trunk will be used to route SIP calls to Avaya SES that are destined for Exchange Pro.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Signaling Group
Create a new SIP signaling group using the add signaling-group n command, where n is the number of an unused signaling group. Use the same parameters as shown in Section 4.1, Step 3 for signaling group 1 with the following exception. Set the Far-end Domain field to the IP address of Exchange Pro. The compliance test used signaling group 18 as shown below.
<pre>
add signaling-group 18   Page   1 of 1
                                SIGNALING GROUP

 Group Number: 18   Group Type: sip
                        Transport Method: tls

   Near-end Node Name: procr   Far-end Node Name: SES
 Near-end Listen Port: 5061   Far-end Listen Port: 5061
                                        Far-end Network Region: 1
       Far-end Domain: 10.75.5.29

                                             Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload   Direct IP-IP Audio Connections? y
                                                       IP Audio Hairpinning? n
         Enable Layer 3 Test? n
 Session Establishment Timer(min): 3   Alternate Route Timer(sec): 6
</pre></td></tr>
</table>

Step	Description
2.	**Trunk Group** Create a new trunk group using the **add trunk-group *n*** command, where ***n*** is the number of an unused trunk group. Use the same parameters as shown in **Section 4.1**, **Steps 4 - 5** for trunk group 1 with the following exceptions. Use unique values for the **Group Name** and **TAC** fields. Set the **Signaling Group** field to the signaling group number created in the previous step. The compliance test used trunk group 18 with the following values. ▪ **Group Name**: ***ExchangePro*** ▪ **TAC**: ***118*** ▪ **Signaling Group**: ***18***
3.	**Public Unknown Numbering** Public unknown numbering defines the calling party number to be sent to the far-end. The entry created in **Section 4.1**, **Step 6** applies to all trunks since the **Trk Grp** column was left blank. Thus, a separate entry does not need to be created for this new SIP trunk. Based on the previous entry, all calls originating from a 5-digit extension beginning with 3 will be sent as a 5-digit calling number. This calling party number is sent to the far-end in the SIP "From" header.
4.	**Automatic Route Selection (ARS)** Automatic Route Selection (ARS) was used to route outbound calls to the PSTN via the Exchange Pro. To dial PSTN numbers, enterprise users would first dial the ARS access code followed by the PSTN number. PSTN numbers beginning with 1732 were used for the compliance test. Use the **change ars analysis** command to create an entry in the ARS Digit Analysis Table to route 11-digit numbers beginning with 1732 to route pattern 18. Route pattern 18 will direct the call to the Exchange Pro trunk group (see **Step 5**).

Step 2 screen:

```
add trunk-group 18                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 18                  Group Type: sip           CDR Reports: y
  Group Name: ExchangePro                COR: 1        TN: 1        TAC: 118
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n

                                                     Signaling Group: 18
                                                   Number of Members: 10
```

Step 4 screen:

```
change ars analysis 1732                                        Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    3

          Dialed           Total     Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    1732                  11   11    18        fnpa         n
```

Step	Description
5.	**Route Pattern** Create a route pattern for use by ARS when routing calls to the PSTN via the Exchange Pro. The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern n** command, where ***n*** is the number of an unused route pattern to configure the parameters in the following manner. The example below shows the values used for the compliance test. ▪ **Pattern Name**: Enter a descriptive name. ▪ **Grp No**: Enter the outbound trunk group for the Exchange Pro defined in **Step 2**. ▪ **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level. ▪ **Pfx Mrk**: Set the Prefix Mark to ***1***. This will prepend a 1 to any 10-digit numbers and leave numbers of any other length unchanged. This was not strictly necessary for the compliance test since only 11-digit PSTN dialing was tested. However, using a Prefix Mark of 1 is common practice when routing calls to the PSTN. ▪ **Inserted Digits**: ***00*** The Exchange Pro requires the prefix of 00 be inserted in front of the dialed number when directing a call to the PSTN. ▪ Default values can be used for all other fields.

```
change route-pattern 18                                           Page   1 of   3
                    Pattern Number: 18  Pattern Name: ExchangePro
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 18   0       1                00                                   n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                         none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

Step	Description
6.	**Automatic Alternate Routing (AAR)** Automatic Alternate Routing (AAR) was used to route outbound calls to Skype users via the Exchange Pro. To dial the Skype users, enterprise users would first dial the AAR access code followed by the number assigned to the Skype user. For the compliance test, 2-digit numbers beginning with 2 were assigned to the Skype users. Use the **change aar analysis** command to create an entry in the AAR Digit Analysis Table to route 2-digit numbers beginning with 2 to route pattern 21. Route pattern 21 will direct the call to the Exchange Pro trunk group (see **Step 5**).

```
change aar analysis 2                                         Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location:  all           Percent Full:    3

          Dialed            Total      Route     Call   Node   ANI
          String          Min  Max  Pattern    Type   Num    Reqd
    2                     2    2     21        aar           n
```

Step	Description
7.	**Route Pattern** Create a route pattern for use by AAR when routing calls to the Skype users via the Exchange Pro. Create the route pattern in the same manner and using the same values as the route pattern configured in **Step 5** with the following exceptions. ▪ **Pattern Name**: Enter a unique name. ▪ **Pfx Mrk**: Leave the **Pfx Mrk** field blank. There is no need to set the Prefix Mark to 1 in this case since no 10-digit numbers will use this route pattern. ▪ **Inserted Digits**: Leave the **Inserted Digits** field blank. The Exchange Pro does not require any prefix be inserted in front of the dialed number of the Skype users. ▪ Default values can be used for all other fields.

```
change route-pattern 21                                         Page   1 of   3
                    Pattern Number: 21  Pattern Name: ExchangePro2
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 18   0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                         none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
```

Step	Description

8.	**Inbound Calls**
	All calls received from the Exchange Pro have the same destination number. This number is typically configured to be the extension of an automated attendant or other IVR application. This number is configured on the Exchange Pro in the **Trunk Username** field (**Section 6**, **Step 13**). In the case of the compliance test, the vector directory number (VDN) 39100 was used. This VDN will invoke vector 1 when 39100 is dialed. Vector 1 implements a simple automated attendant. To create a VDN, use the **add vdn** command. Enter any descriptive name for the **Name*** field. In the **Vector Number** field, enter the vector number to be invoked (see **Step 9**).
	<pre>add vdn 39100 Page 1 of 3
	                            VECTOR DIRECTORY NUMBER
	
	                             Extension: 39100
	                                 Name*: AutoAttendant
	                         Vector Number: 1
	
	                  Meet-me Conferencing? n
	                    Allow VDN Override? n
	                                   COR: 1
	                                   TN*: 1
	                              Measured: none
	
	               Service Objective (sec): 20
	
	                            1st Skill*:
	                            2nd Skill*:
	                            3rd Skill*:
	
	* Follows VDN Override Rules</pre>

9.	**Automated Attendant Vector**
	Vector 1 was used to provide an automated attendant for incoming calls. The configuration of vector 1 is shown below. A vector can be created with the **change vector** command.
	• **Name**: Any descriptive name
	• Step **01**: Collect 5 digits. No announcement is played.
	• Step **02**: Route the calls to the extension collected in vector step 01 and if necessary proceed to coverage.
	<pre>change vector 1 Page 1 of 6
	                                  CALL VECTOR
	
	    Number: 1 Name: AutoAttendant
	                                            Meet-me Conf? n Lock? n
	     Basic? y EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? n
	 Prompting? y LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
	 Variables? n 3.0 Enhanced? y
	01 collect 5 digits after announcement none
	02 route-to digits with coverage y
	03</pre>

5. Configure Avaya SIP Enablement Services

This section covers the configuration of Avaya SES. Avaya SES is configured via an Internet browser using the administration web interface. It is assumed that the Avaya SES software and the license file have already been installed on the server. During the software installation, an installation script is run from the Linux shell of the server to specify the IP network properties of the server along with other parameters. In addition, it is assumed that the setup screens of the administration web interface have been used to initially configure Avaya SES. For additional information on these installation tasks, refer to [5].

Each SIP endpoint used in the compliance test that registers with Avaya SES requires that a user and media server extension be created on Avaya SES. This configuration is not directly related to the interoperability of Exchange Pro so it is not included here. These procedures are covered in [5].

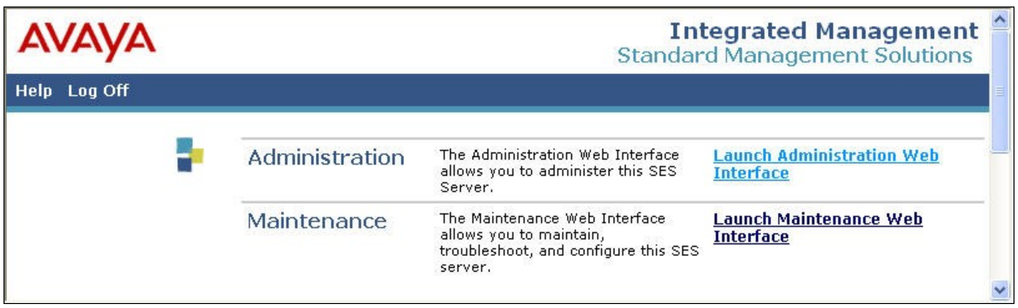
This section is divided into two parts. **Section 5.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. It will not attempt to show the installation procedures in their entirety. It will also describe any deviations from the standard procedures, if any.

Section 5.2 will describe procedures beyond the initial SIP installation procedures that are necessary for interoperating with Exchange Pro.

5.1. Summarize Initial Configuration Parameters

This section summarizes the applicable user-defined parameters used during the SIP installation procedures.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Login
Access the Avaya SES administration web interface by entering http://<<i>ip-addr</i>>/admin as the URL in an Internet browser, where <<i>ip-addr</i>> is the IP address of the Avaya SES server.

Log in with the appropriate credentials and then select the Launch Administration Web Interface link from the main page as shown below.

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>

Top Page
The Avaya SES **Top** page will be displayed as shown below.

</td></tr>
<tr><td>3.</td><td>

Initial Configuration Parameters
As part of the Avaya SES installation and initial configuration procedures, the following parameters were defined. Although these procedures are out of the scope of these Application Notes, the values used in the compliance test are shown below for reference. After each group of parameters is a brief description of how to view the values for that group from the Avaya SES administration home page shown in the previous step.

- SIP Domain: ***business.com***
  (To view, navigate to **Server Configuration→System Parameters**)

- Host IP Address (SES IP address): ***10.75.5.6***
- Host Type: ***SES combined home-edge***
  (To view, navigate to **Host→List**; click **Edit**)

- Communication Manager Server Interface Name: ***CMeast***
- SIP Trunk Link Type: ***TLS***
- SIP Trunk IP Address (Avaya S8300 Server IP address): ***10.75.5.2***
  (To view, navigate to **Communication Manager Server→List**; click **Edit**)

</td></tr>
</table>

5.2. Exchange Pro VISIP-EX Specific Configuration

This section describes additional Avaya SES configuration necessary for interoperating with Exchange Pro.

Step	Description
1.	**Trusted Host** Define the Exchange Pro to be a trusted host. Navigate to **Trusted Hosts→Add** in the left pane. In the **Add Trusted Host** window that appears, configure the following: • **IP Address**: Enter the IP address of the Exchange Pro. • **Host**: Select the Avaya SES IP address from the drop-down menu. • **Comment**: Enter a description of the trusted host being added. Click the **Add** button. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>Communication Manager Server Address Maps
A Communication Manager Server Address Map is needed to route calls from the Exchange Pro to Avaya Communication Manager. Thus to accomplish this task, a Communication Manager Server Address Map is needed.

To view the configured Communication Manager Server Address Maps, navigate to Communication Manager Server→List in the left pane. In the window that appears (not shown), click the Map link next to the Communication Manager Server name. The list of address maps will appear. Each map defines criteria for matching calls to Avaya SES based on the contents of the SIP Request-URI of the call. If a call matches the map, then the call is directed to the Contact.

In the example below, the single map used for the compliance test is shown. This map was associated to a Contact that directs the calls to the IP address of the Avaya Communication Manager (10.75.5.2) using port 5061 and TLS as the transport protocol. The user portion in the original request URI is substituted for $(user)</i> in the Contact expression shown below.

<code>sip:$(user)@10.75.5.2:5061;transport=tls</code>

This contact is created automatically after the first map is created. The map was originally created by selecting the Add Map In New Group link. To view or edit the call matching criteria of the map, click the Edit link next to the map name.


</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>

Address Maps – Continued
The content of the address map is described below. This map is used to route the incoming 39100 extension from the Exchange Pro to Avaya Communication Manager. Extension 39100 is the destination address for all incoming Skype calls. This extension must match the trunk **Username** configured on the Exchange Pro in **Section 6**, **Step 13**.

- **Name**: Contains any descriptive name
- **Pattern**: Contains an expression to define the matching criteria for calls to be routed from the Exchange Pro to Avaya Communication Manager. For the address map named ***ToMainCM***, the expression will match any URI that begins with ***sip:3*** followed by any digit between ***0-9*** for the next ***4*** digits. Additional information on the syntax used for address map patterns can be found in [5].
- **Replace URI**: Check the box.

If any changes are made, click **Update**.

</td></tr>
</table>

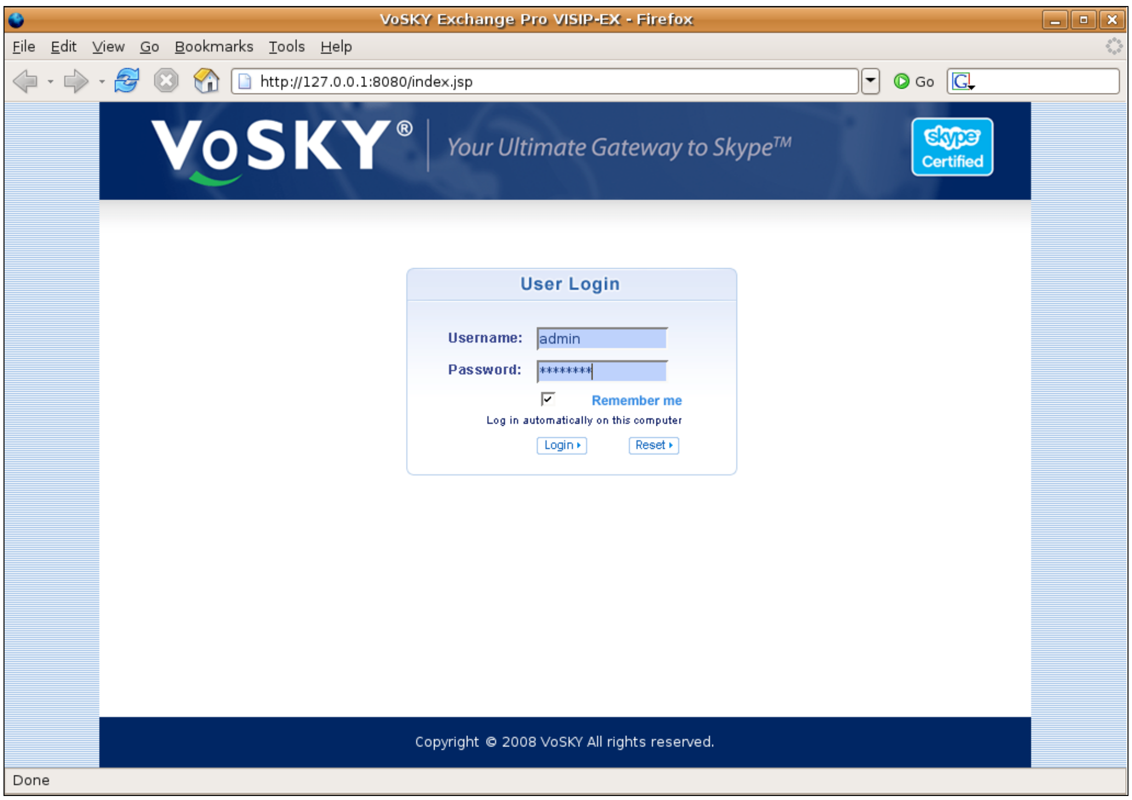
6. Configure Exchange Pro VISIP-EX

This section describes the configuration of the Exchange Pro. The Exchange Pro is configured via a web interface and can be accessed with a web browser either external or internal to the Exchange Pro server. If external to the Exchange Pro server, enter **http://<*ip-addr*>:8080/index** as the destination address in a web browser where <*ip-addr*> is the IP address of the Exchange Pro. If internal to the Exchange Pro server, launch the browser from the Linux GNOME desktop environment. The default home page points to the configuration web interface.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

Login

On the initial **Login** page, enter a proper **Username** and **Password**. Click **Login**.

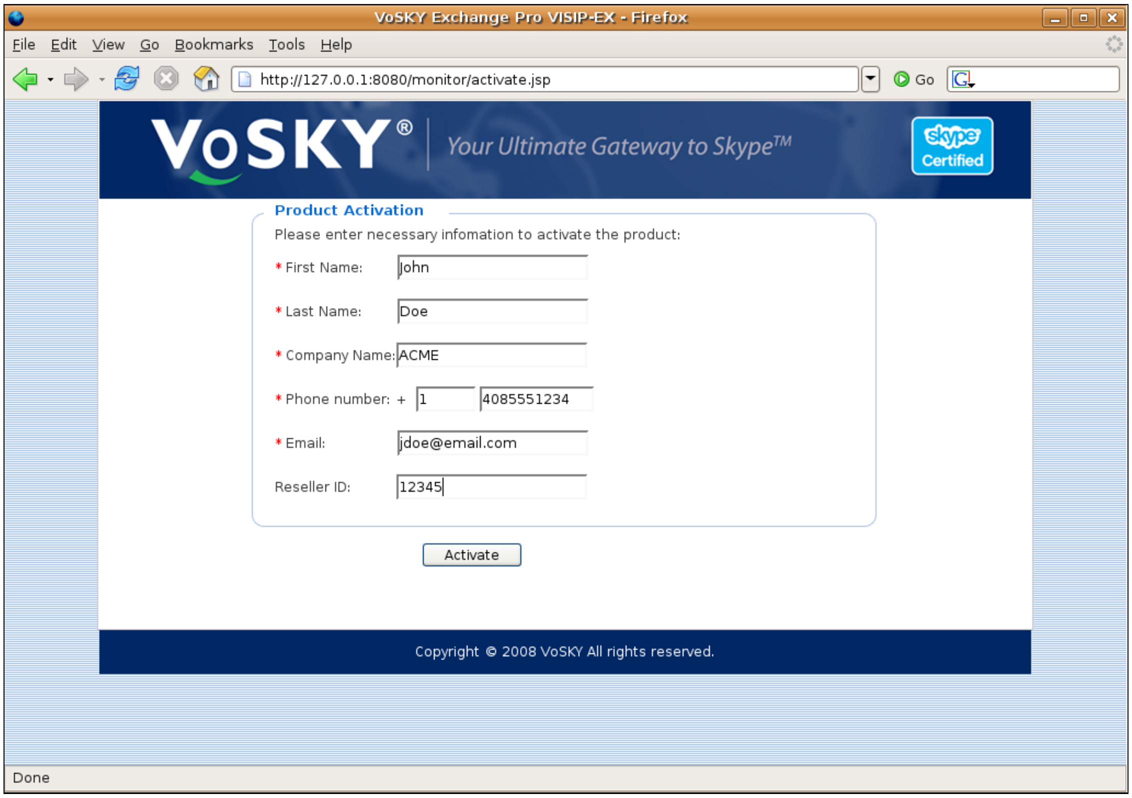


</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>

Product Activation

The first time the web interface is accessed, the following **Product Activation** screen will appear. Enter all required fields indicated by a *, then click **Activate**.

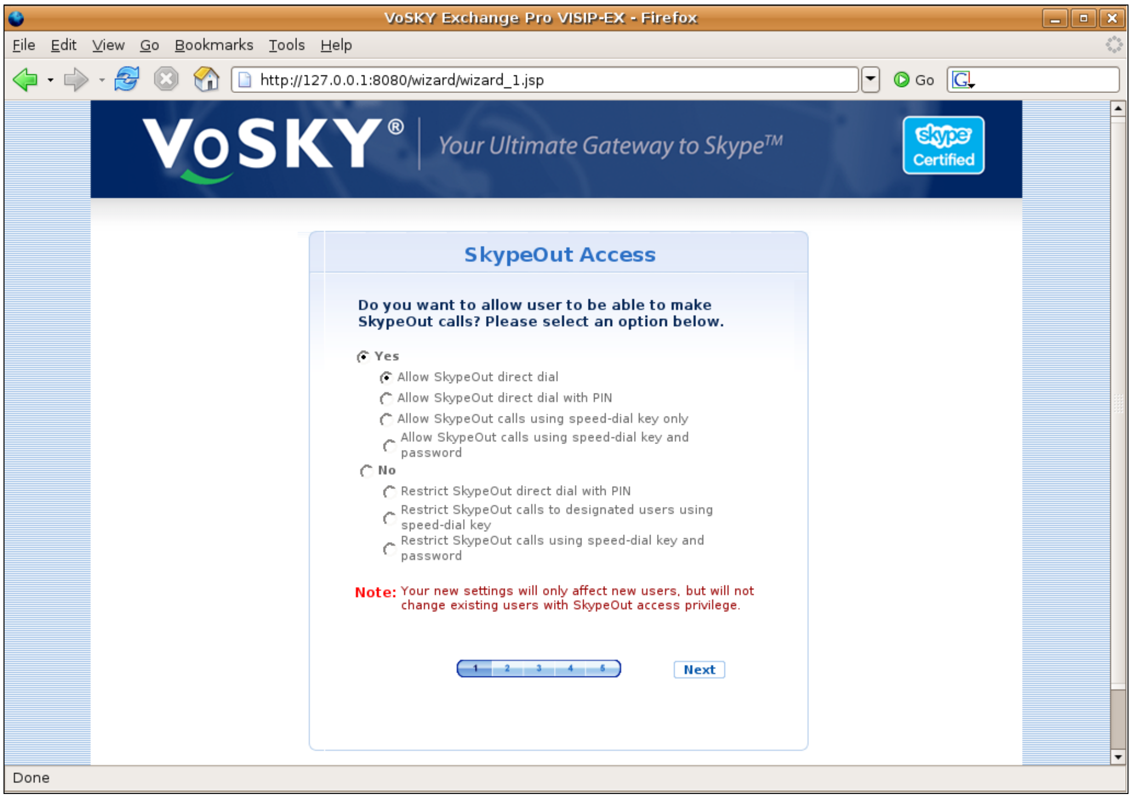


</td></tr>
</table>

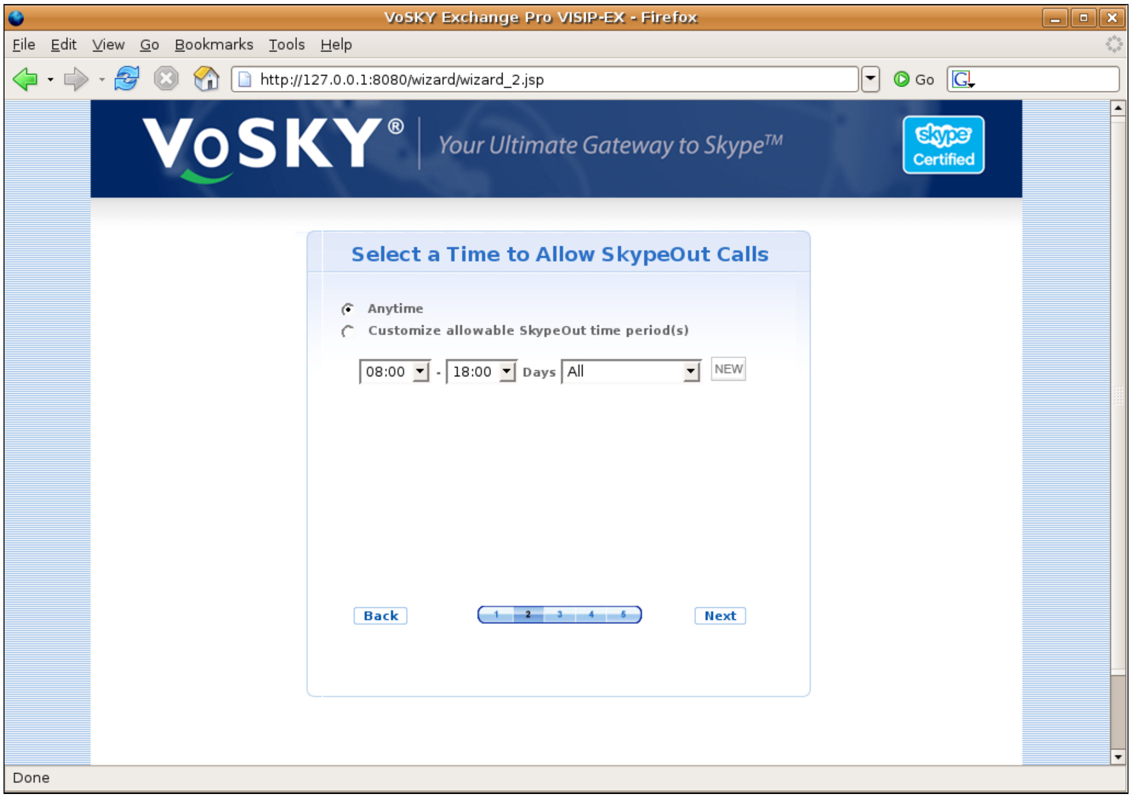
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>

SkypeOut Access

At this point, the configuration wizard will start automatically with the **SkypeOut Access** screen shown below. Select the appropriate options then click **Next** to proceed. For the compliance test, users were allowed to make outbound Skype calls. Thus, the **Yes** option was selected followed by the **Allow SkypeOut direct dial** option. This allows users to dial the outbound number directly without requiring a PIN, speed-dial key or password.



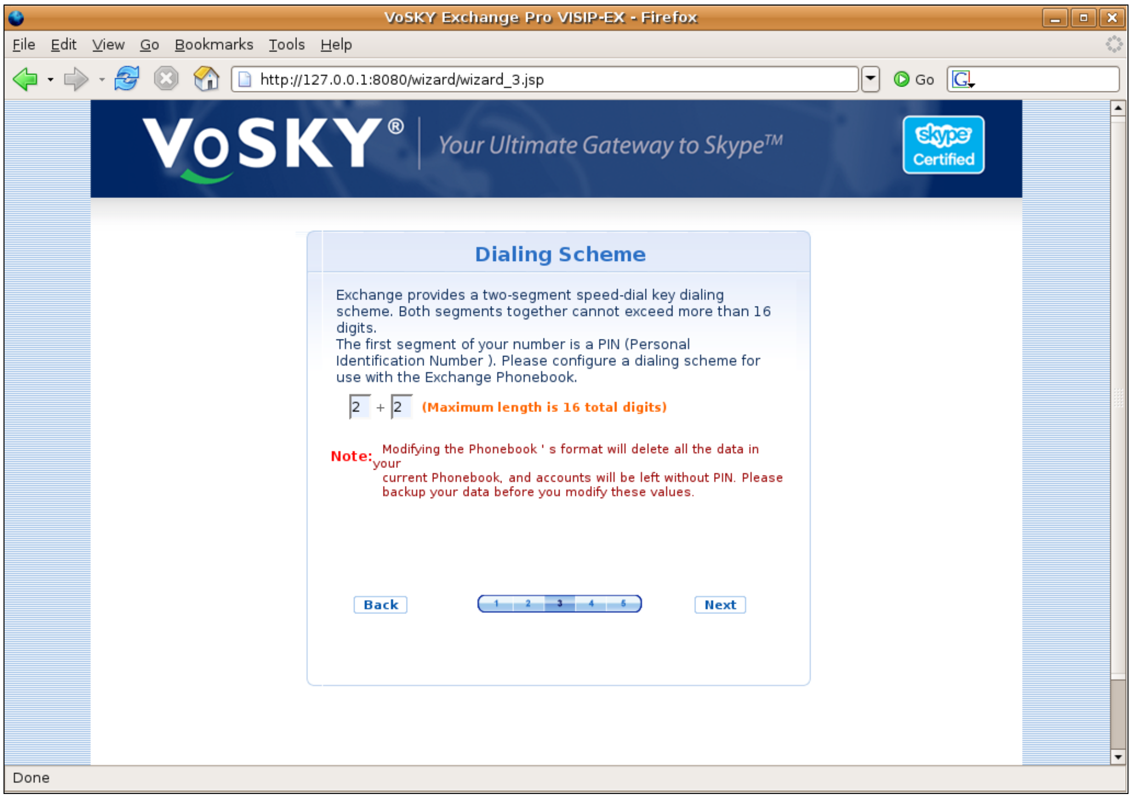
</td></tr>
</table>

Step	Description
4.	**Time Outbound Calls Are Available** Select which days and what time of day to allow outbound calls. Click **Next** to proceed. For the compliance test, the **Anytime** option was selected. 

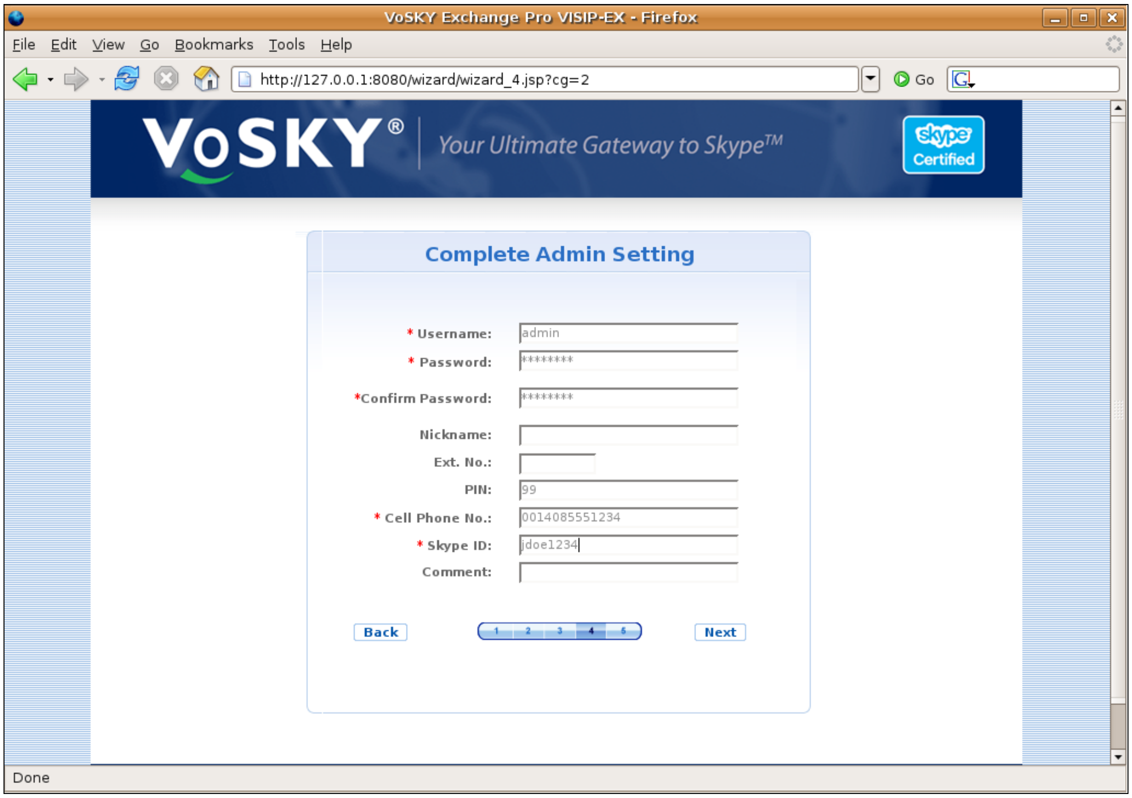
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.</td><td>

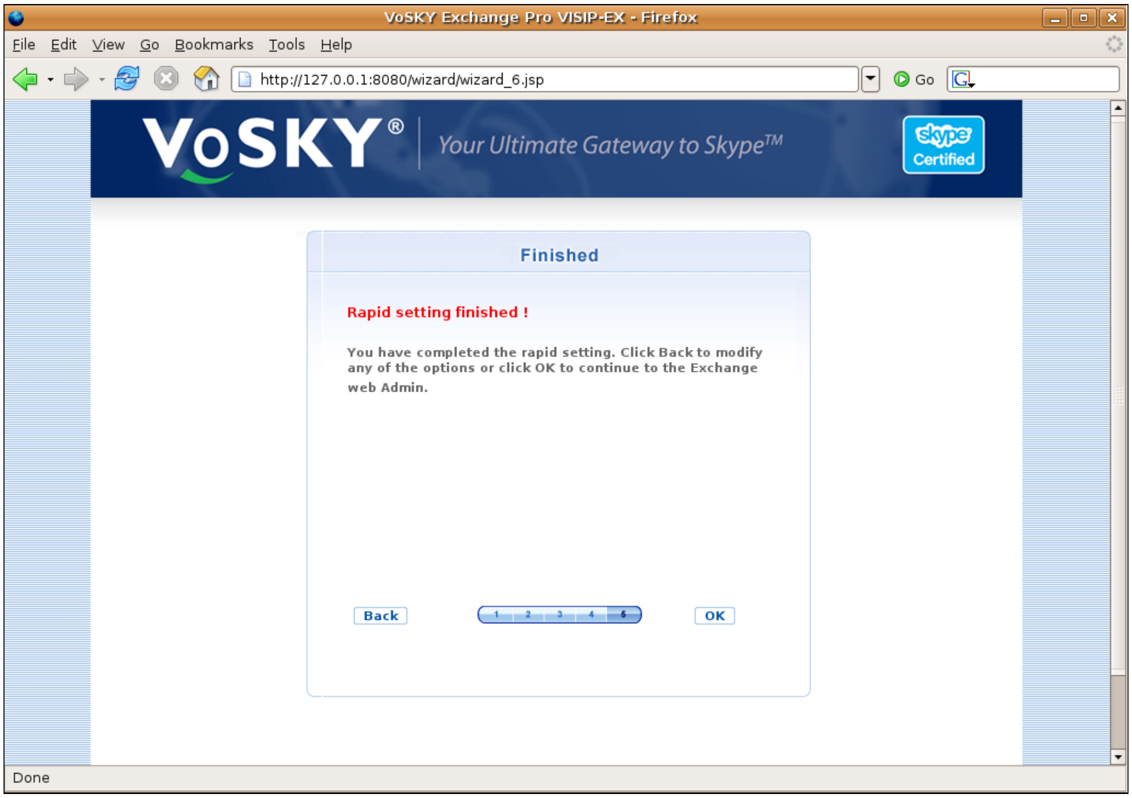
Dialing Scheme

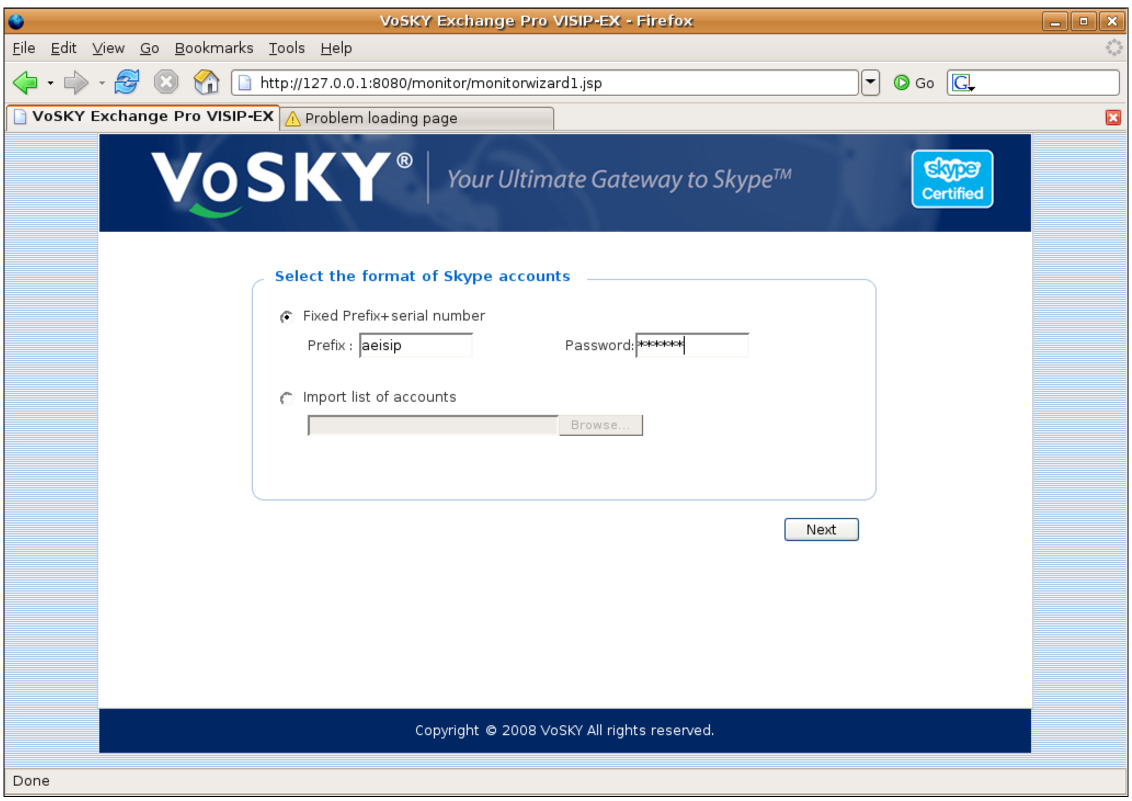
Define the dialing scheme for the speed-dial codes used to dial other Skype users. The speed-dial is comprised of a PIN (if required) plus the dialed string assigned to a particular user. Enter the digit length of the PIN in the first box and the digit length of the user code in the second box. For the compliance test, a 2-digit PIN and a 2-digit user code were defined. However, since a PIN is not required (as defined in **Step 3**) then all Skype users in the Exchange Pro phone book can be reached by dialing a 2-digit code.



</td></tr>
</table>

Step	Description
6.	**Admin Settings** The **Complete Admin Setting** page that appears shows the default settings for the Exchange Pro administrator account. Enter any missing or incorrect information in the required fields marked with a *. The cell phone number (**Cell Phone No.**) and **Skype ID** is the administrator contact information. Click **Next** to proceed. 

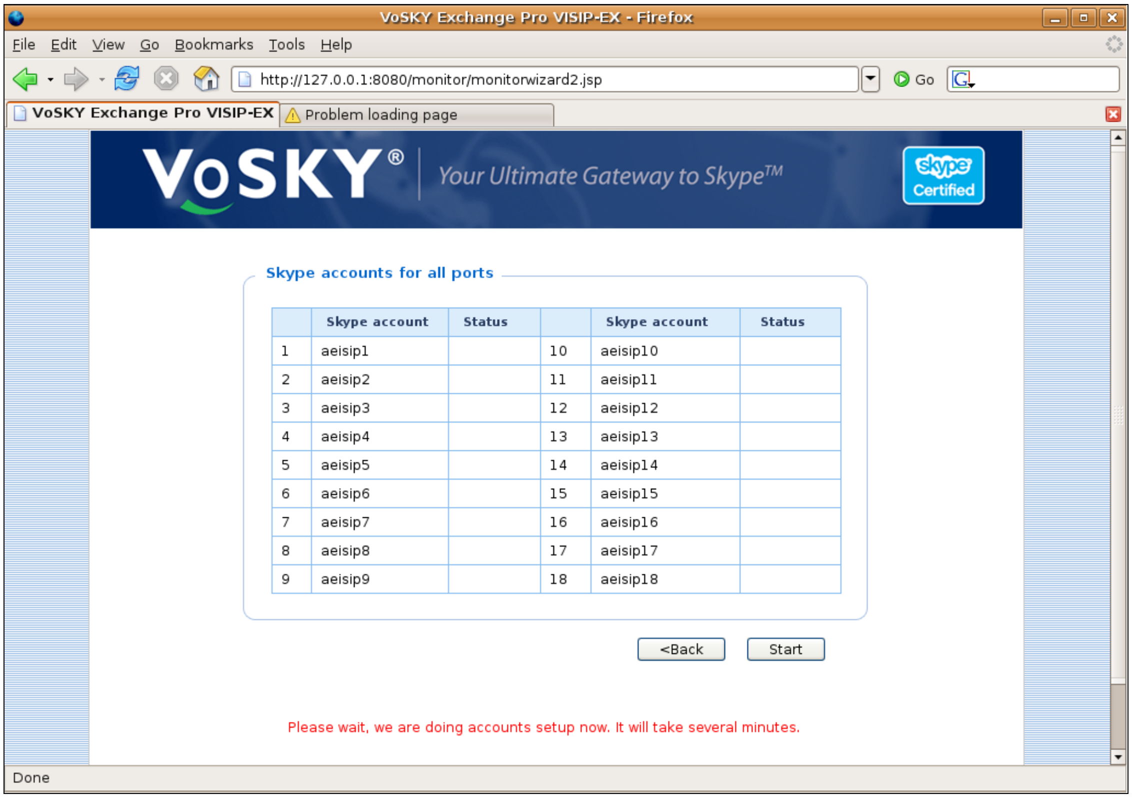
Step	Description
7.	**Wizard Setup Complete** The **Finished** screen appears as shown below. Click **OK** to proceed to the Exchange Pro web administration. 

Step	Description
8.	**Account Format** Define the format of the Skype account names used by the Exchange Pro. Prior to Exchange Pro installation, the customer has been instructed to sign-up with the Skype service and obtain a set of accounts, one account for each license purchased with Exchange Pro. The customer selects the account names (Skype IDs) for these accounts so they may have a common format. If the accounts have a common format, it can be specified here. Otherwise, the account names can be imported in a list. One account is used for each active call involving the Exchange Pro. Thus, the number of accounts also represents the number of simultaneous calls supported by the Exchange Pro. In the case of the compliance test, each account started with the same prefix followed by a number. Thus, the **Fixed Prefix + serial number** option was selected. Enter the prefix in the **Prefix** field (*aeisip*). Enter a password in the **Password** field. All accounts will share the same password. Click **Next** to proceed. Exchange Pro will start the serial number count at 1 and increment it for each available license. The compliance test used 18 licenses. Thus, Exchange Pro set-up accounts aeisip1 through aeisip18. 

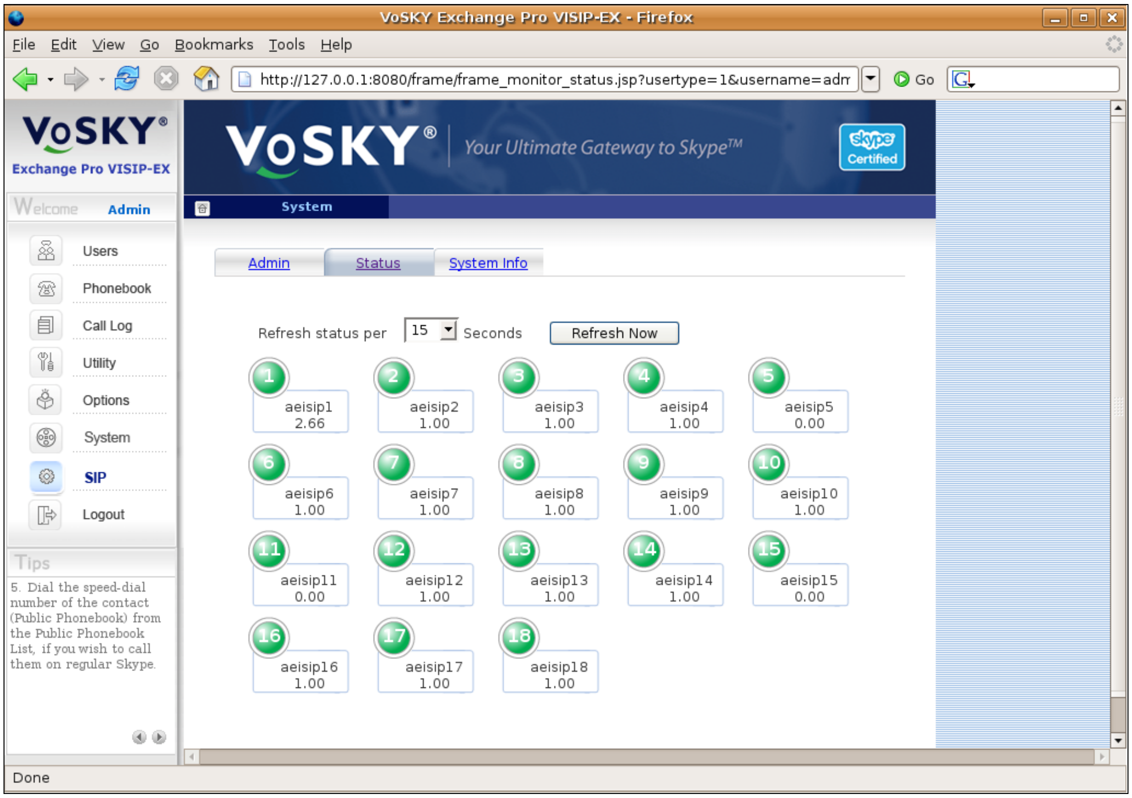
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>9.</td><td>

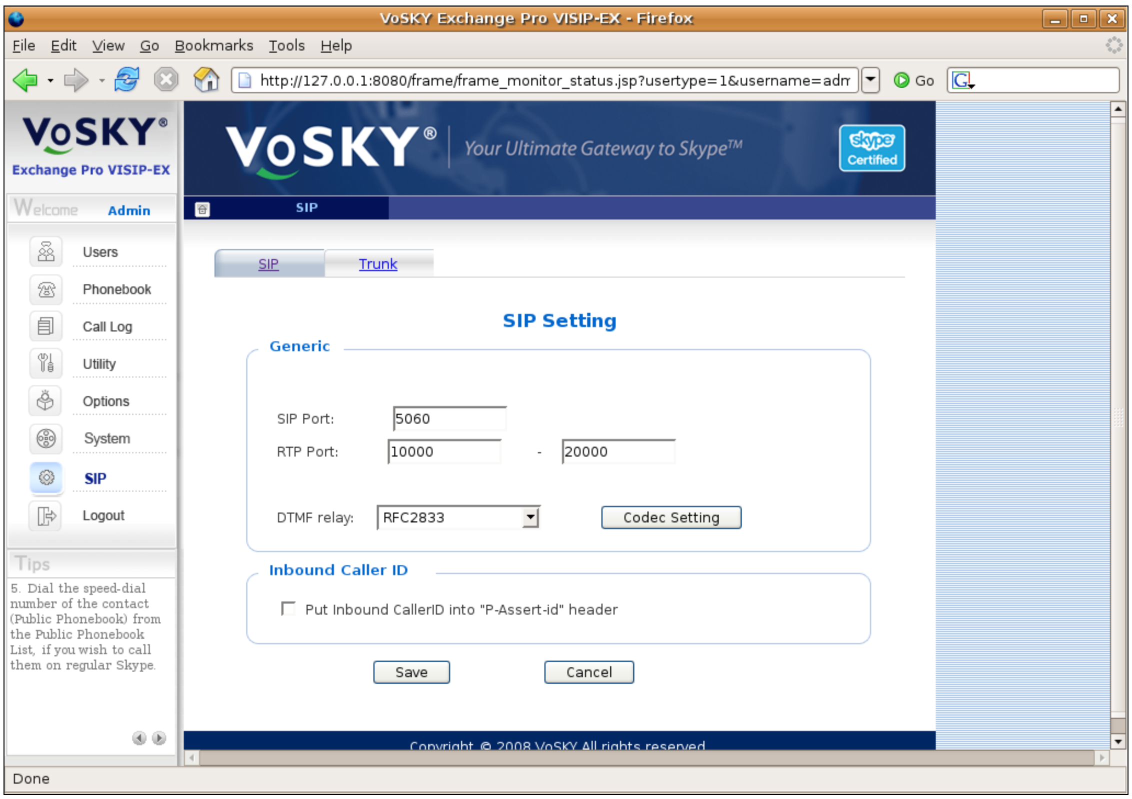
Account List

A status screen appears, while the accounts defined in **Step 8** are being set-up. Once the set-up is complete, click the **Start** button to begin the process of logging in to each Skype account. The full administration GUI will open automatically to finish the configuration.



</td></tr>
</table>

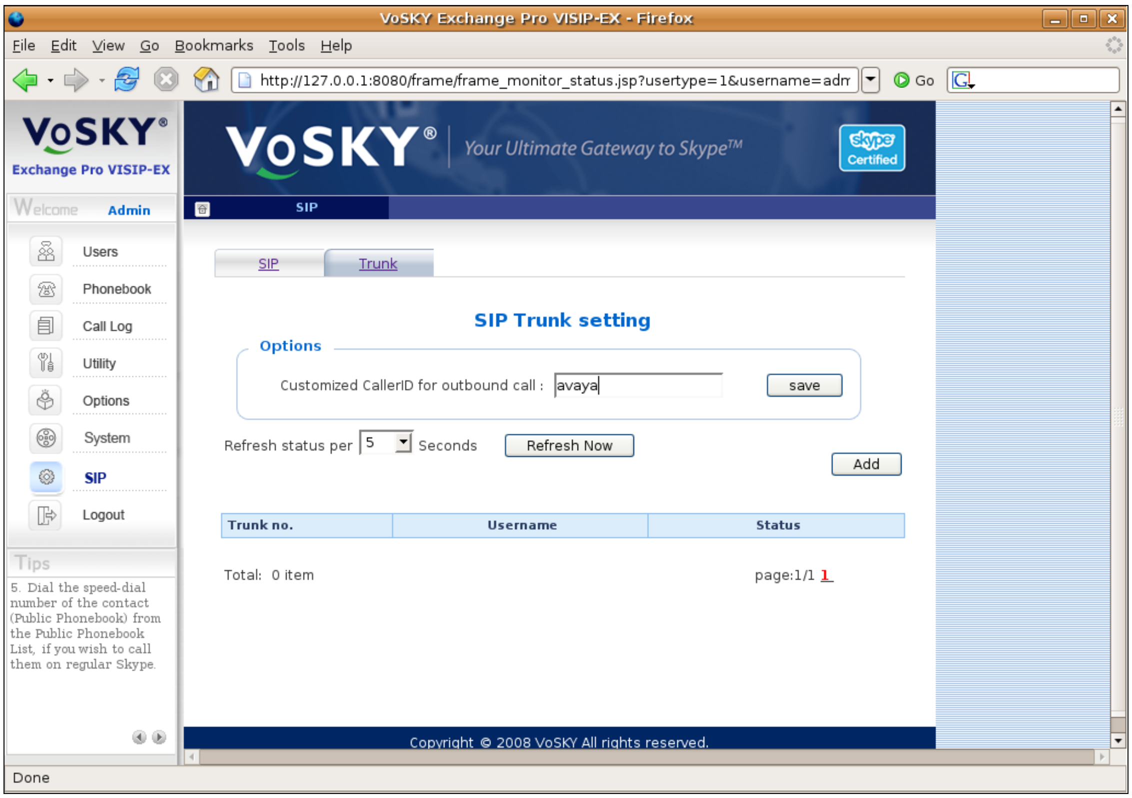
Step	Description
10.	**System Status** The full administration GUI opens with the **Status** tab of the **System** page. It shows the status of each of the accounts previously created. The green light next to each account name indicates Exchange Pro was successfully able to log in to the Skype service with that account. 

Step	Description
11.	**General SIP Settings** To configure the SIP settings, click the **SIP** link in the left pane of the window. On the **SIP** tab, set the following parameters as shown below. Click **Save**. ▪ **SIP Port**: ***5060*** This is the standard SIP port. ▪ **RTP Port:** Enter a start port and end port to define a range of RTP ports that the Exchange Pro will listen on for RTP traffic. ▪ **DTMF relay: RFC2833** This instructs the Exchange Pro to use RTP events to send DTMF tones as defined in RFC2833. 

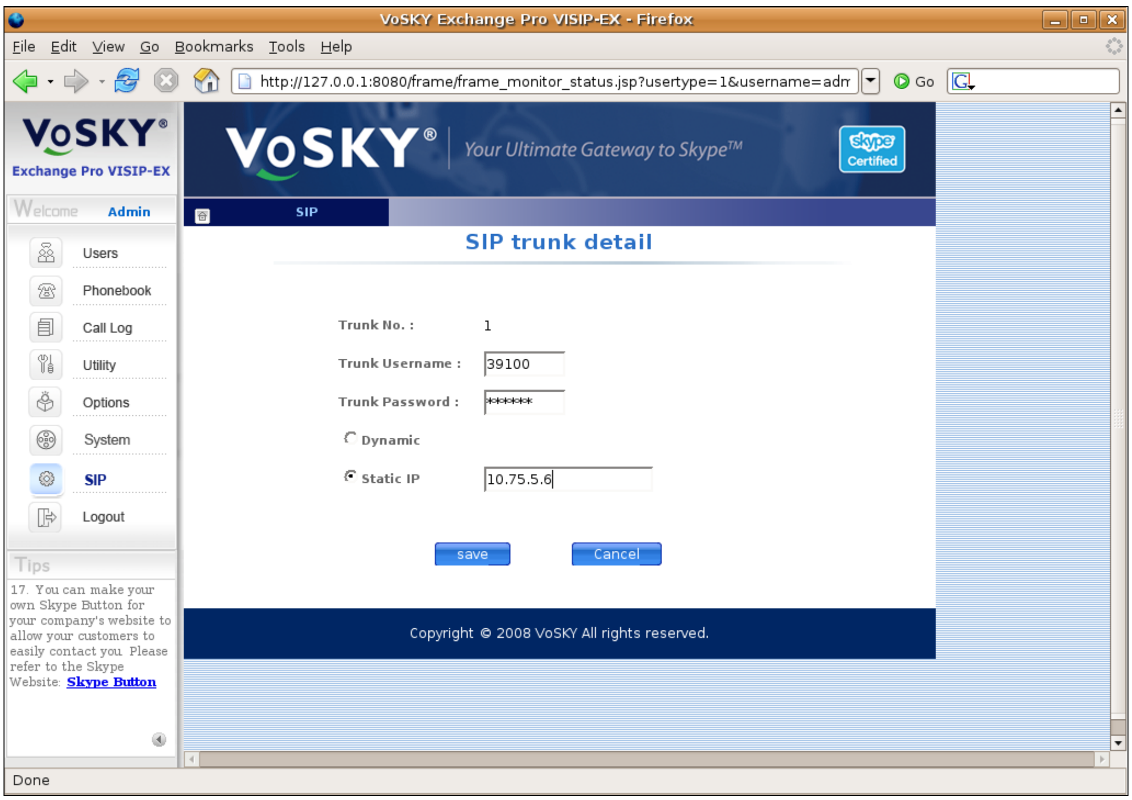
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>12.</td><td>

SIP Trunk

Click the **Trunk** tab. In the **Customized CallerID for outbound call** field, enter a descriptive name then click **save**. This name will be used as the caller's name in outbound calls from the Exchange Pro to the Skype clients. This value is not used for Skype calls to the PSTN. Skype does not support Caller ID. Thus, in the case of calls to the PSTN, Skype inserts an arbitrary defined number as the caller party name. Click the **Add** button to create the trunk details for the connection to Avaya SES.

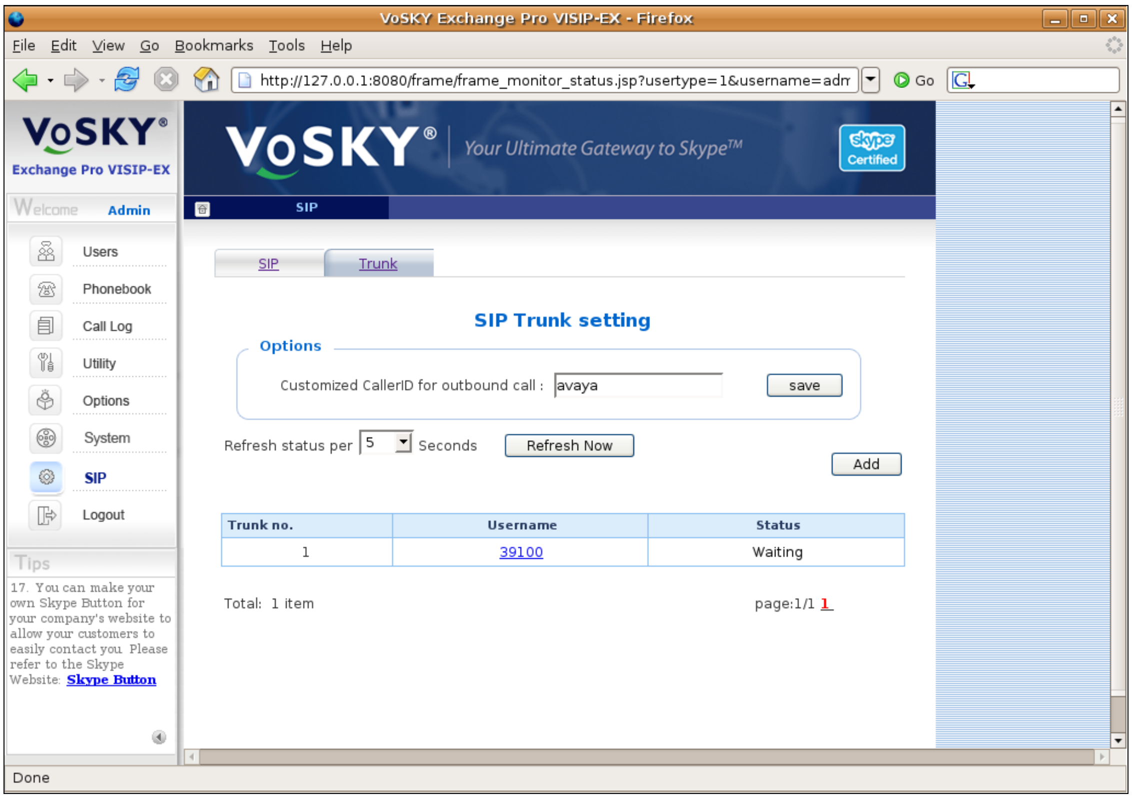


</td></tr>
</table>

Step	Description
13.	**SIP Trunk Detail** Enter the trunk parameters as described below, then click **save**. ▪ **Trunk Username**: Enter a dial string. This string will appear as the user part of the SIP "To" header for inbound calls to Avaya SES and ultimately Avaya Communication Manager. This dial string is used by Avaya Communication Manager to route the call to the final destination. The Exchange Pro will use this dial string as the destination address for all inbound calls from the Skype network. In the case of the compliance test, the extension of the automated attendant created in **Section 4.2**, **Step 8** was entered in this field. ▪ **Trunk Password:** Enter any password accepted by Exchange Pro. This value is not used by Avaya Communication Manager. ▪ **Static IP:** Enter the IP address of the Avaya SES. 

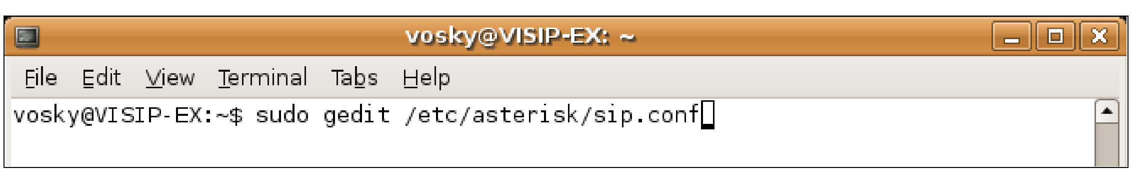
Step	Description
14.	**SIP Trunk User**

Once the trunk details have been configured, the trunk and its **Username** and **Status** appears at the bottom of the Trunk tab. The example below shows the trunk used for the compliance test. The **Status** is shown as ***Waiting*** since it had just been configured and was still coming into service. This completes the configuration accessible via the configuration GUI.



Step	Description
15.	**Edit Configuration File**

The Exchange Pro SIP configuration is stored in the sip.conf file on the Exchange Pro server. After completing the above configuration, additional configuration changes are required to this file which can not be done from the web interface. Thus, the sip.conf file must be edited directly. To edit this file, begin by opening a terminal window on the Exchange Pro Linux server by using the GNOME desktop interface to navigate to **Applications → Accessories → Terminal**. In the terminal window that appears, type the command “sudo gedit /etc/asterisk/sip.conf” to edit the sip.conf file as shown below.

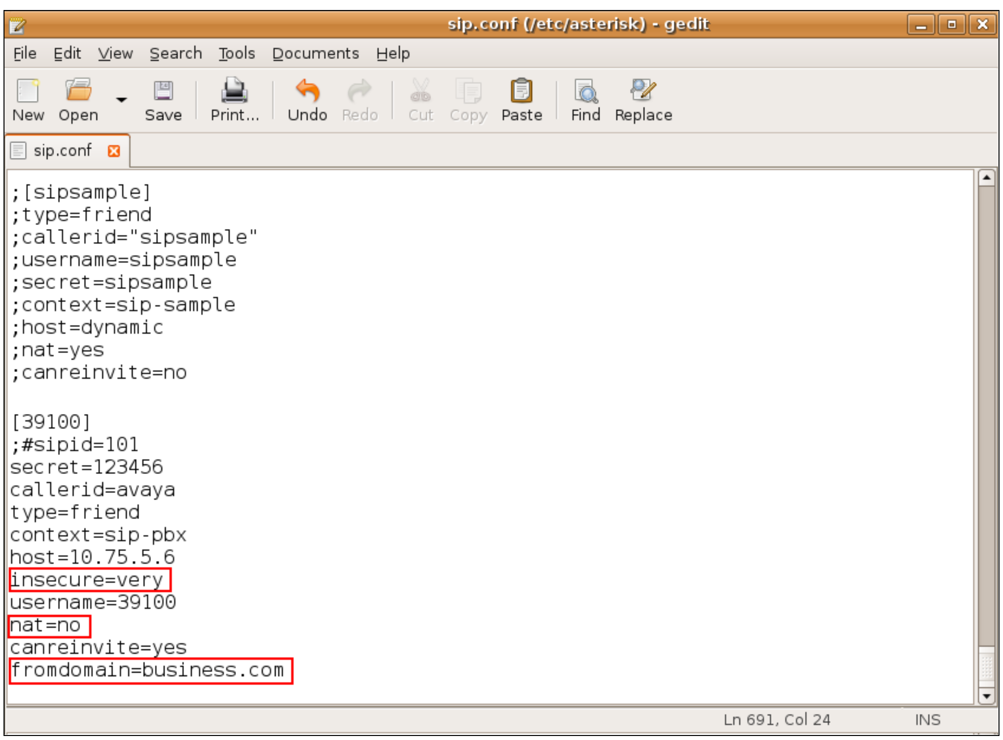


<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>16.</td><td>

Edit Configuration File

Locate the section of the file containing the trunk parameters. This section will begin with a line containing the trunk username in brackets. In the case of the compliance test, this is the section starting with *[39100]*. Configure the parameters as described below. Click **Save**, followed by **File→Exit** to save the modified file.

- Set **insecure=*very***. This will disable trunk username and password authentication. The Avaya SES supports authentication of SIP users but not authentication of trunk connections. Instead, the Exchange Pro is configured as a trusted host on Avaya SES (**Section 5.2**, **Step 1**).
- Set **nat=*no***. This will ensure that the Exchange Pro sends all SIP traffic to port 5060 and not try to use the Avaya Communication Manager source port for SIP traffic.
- Set **fromDomain** to match the **Far-end Domain** field of one of the Avaya Communication Manager SIP signaling groups. For the compliance test, the **fromDomain** was set to the SIP domain of Avaya SES and matches the **Far-end Domain** field of trunk 1 (**Section 4.1**, **Step 3**). Thus, all inbound traffic to Avaya Communication Manager used trunk 1. However, a more common approach would be to set the **fromDomain** to the IP address of the Exchange Pro used in the **Far-end Domain** field for trunk 18 (***10.75.5.29***) in **Section 4.2**, **Step 1**. This way the same trunk (trunk 18) would be used for both outbound and inbound traffic between Avaya Communication Manager and the Exchange Pro.



</td></tr>
</table>

7. General Test Approach and Test Results

The interoperability compliance testing consisted of placing calls through the Exchange Pro and exercising common PBX features. Calls were placed between the Avaya Communication Manager endpoints and the Skype users; as well as between the Avaya Communication Manager endpoints and the Skype-connected PSTN.

Exchange Pro passed compliance testing. The following features and functionality were verified. Any observations related to these tests are listed at the end of this section.

- Calls between an Avaya Communication Manager endpoint and a Skype user.
- Calls between an Avaya Communication Manager endpoint and a PSTN user via the Exchange Pro.
- Interoperability of the Exchange Pro with analog, digital, H.323, and SIP telephones.
- Interoperability of the Exchange Pro with Avaya one-X Desktop Edition (SIP soft client).
- G.711mu codec support.
- Proper recognition of DTMF transmissions by navigating voicemail menus.
- Voicemail support.
- PBX features including Hold, Transfer, Call Waiting, Call Forwarding and Conference.
- Proper system recovery after an Exchange Pro restart and loss of IP connection.

The following observations were made during the compliance test:

- If an enterprise user calls the PSTN and the called party is "busy", the caller does not hear busy tone and the call is dropped. This was attributed to the operation of Skype and not related to an issue with interoperability between Exchange Pro and Avaya Communication Manager and Avaya SIP Enablement Services.
- Incoming Caller ID – When calling from an Internet Skype endpoint, the called party at the enterprise sees the caller's name preceded by an unexpected character. When calling from the PSTN, the Exchange Pro sends 000000 as the calling number since the SkypeIN™ service does not support caller ID.

8. Verification Steps

The following steps may be used to verify the configuration:

- From the Avaya Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- Verify that calls can be placed between an Avaya Communication Manager endpoint and a Skype user.
- Verify that calls can be placed between an Avaya Communication Manager endpoint and a PSTN phone via the Exchange Pro.

9. Conclusion

These Application Notes describe the configuration required for VoSKY Exchange Pro VISIP-EX to successfully interoperate with Avaya Communication Manager and Avaya SIP Enablement Services. VoSKY Exchange Pro VISIP-EX successfully passed compliance testing.

10. Additional References

[1] *Feature Description and Implementation For Avaya Communication Manager*, Doc # 555-245-205, Issue 6.0, January 2008.
[2] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 4, January 2008.
[3] *SIP support in Avaya Communication Manager Running on the Avaya S8xxx Servers,* Doc # 555-245-206, Issue 8, January 2008.
[4] *Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide Release 3.0*, version 6.0, Doc # 210-100-500, Issue 9, June 2005
[5] *Installing, Administering, Maintaining, and Troubleshooting SIP Enablement Services*, Doc # 03-600768, Issue 6, June 2008.
[6] *Avaya IA 770 INTUITY AUDIX Messaging Application,* Doc # 11-300532, May 2005.
[7] *4600 Series IP Telephone LAN Administrator Guide*, Doc # 555-233-507, July 2008.
[8] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Installation and Maintenance Guide Release 2.0*, Doc # 16-601943, Issue 2, December 2007.
[9] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide Release 2.0*, Doc # 16-601944, Issue 2, December 2007.
[10] *Avaya one-X Desktop Edition Administration*, October 2006.
[11] *Avaya one-X Desktop Edition Release 2.1 Quick Setup Guid*e, Doc # 16-600974, Issue 2, October 2006.
[12] *Avaya one-X Desktop Edition Getting Started, Doc # 16-600973, Issue 2, September 2007.*
[13] *VoSKY Exchange Pro VISIP-EX User Manual, Version 1.0*

Product documentation for Avaya products may be found at http://support.avaya.com.
Product documentation for Exchange Pro VISIP-EX may be obtained from VoSKY.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.